A kiberbűnözés kora 2025

Nemes Máté

Igazgató

Security Solutions

Mastercard

KiberPajzs
Védelem a pénzügyekben

A kiberbűnözés kora 2025

A Kiberpajzzsal együttműködésben készült tanulmányunk célja, hogy átfogó **tudást és gyakorlati javaslatokat** nyújtson a **védelmi oldal valamennyi szereplőjének**, hozzájárulva ezzel egy **ellenállóbb ökoszisztéma kialakításához**.

Lakossági problémák feltárása

Kvantitatív kutatás:
1000 fős reprezentatív online kutatás a magyar lakosság körében elméleti és gyakorlati feladatokkal.

Adatrendszerezés:
A MÁTRIX projekt keretében publikált rendőrségi bejelentések kategorizálása a digitális csalások típusai és az elszenvedett károk alapján.

Üzleti problémák feltárása

Mastercard Cyber Insights:
Széleskörű iparági elemzés Mastercard adatok felhasználásával.

Szakértői interjúk:
Interjúk üzleti döntéshozókkal, kiberbiztonsági szakértőkkel és rendvédelmi szereplőkkel.

KiberPajzs
Védelem a pénzügyekben

A kiberbűnözés nem különbözik más bűncselekményektől: amíg pénzt termel, folyamatosan növekedni fog – és a becslések szerint 2028 végére az okozott károk globálisan elérhetik a 14000 milliárd dollárt.

14000 milliárd

Becslések szerint 2028-ra a kiberbűnözésből fakadó károk elérhetik a 14000 milliárd dollárt.

30000 millió FT

Magyarországon 2023-ban a kiberbűnözés legalább 30000 millió forintnyi veszteséget okozott.

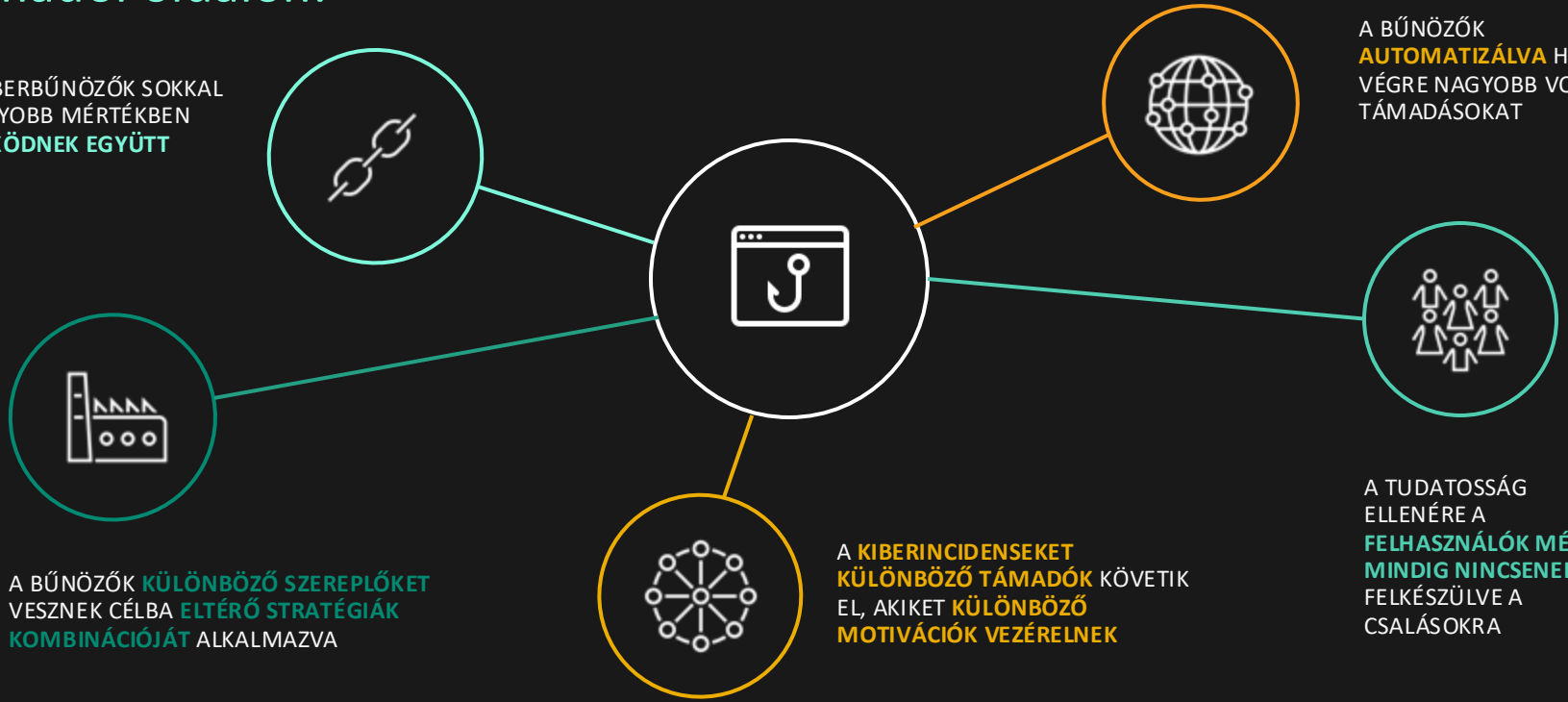
„A kiberbűnözők végcélja a pénzünk megszerzése. Az adataink, amit ellopnak tőlünk, eszközök ebben a folyamatban, hiszen előbb, vagy utóbb ezeket is monetizálni fogják.”

Marsi Tamás, Igazgatóhelyettes, NBSZ NKI

FORRÁSOK: [1]Global cybercrime estimated cost 2029 | Statista
[2] CLOUDFLARE: SHIELDING THE FUTURE: EUROPE'S CYBER THREAT LANDSCAPE (2024), https://cf-assets.www.cloudflare.com/slt3lc6tev37/75ElqwrRueH9MitWszJLYn/4846ff17abe16ffa1ce286d2bdcfbbb6/Shielding-the-future-europes-cyber-threat-landscape.pdf, [3]NÖVEKEDÉS.HU
MEGJEGYZÉS: *2023-BAN

KiberPajzs
Védelem a pénzügyekben

A kiberfenyegetettség egyre növekszik. Ahhoz, hogy hatékonyan felléphessünk ellene, értenünk kell, hogy milyen változások történnek a támadói oldalon.



A KIBERBŰNÖZŐK SOKKAL NAGYOBB MÉRTÉKBEN **MŰKÖDNEK EGYÜTT**

A BŰNÖZŐK **AUTOMATIZÁLVA** HAJTANAK VÉGRE NAGYOBB VOLUMENŰ TÁMADÁSOKAT

A BŰNÖZŐK **KÜLÖNBÖZŐ SZEREPLŐKET** VESZNEK CÉLBA **ELTÉRŐ STRATÉGIÁK KOMBINÁCIÓJÁT** ALKALMAZVA

A **KIBERINCIDENSEKET KÜLÖNBÖZŐ TÁMADÓK** KÖVETIK EL, AKIKET **KÜLÖNBÖZŐ MOTIVÁCIÓK VEZÉRELNEK**

A TUDATOSSÁG ELLENÉRE A **FELHASZNÁLÓK MÉG MINDIG NINCSENEK** FELKÉSZÜLVE A CSALÁSOKRA

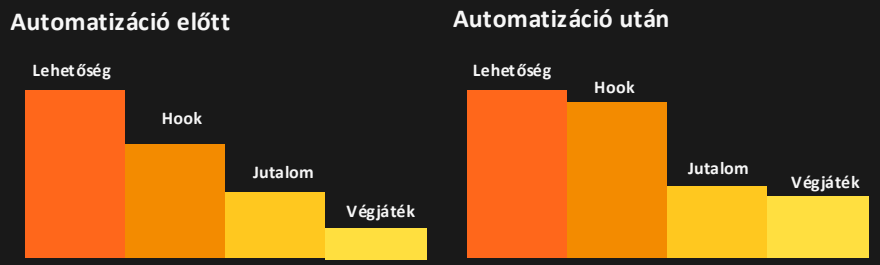
KiberPajzs
Védelem a pénzügyekben

Az AI-alapú automatizálás lehetővé tette a támadók számára nagy mennyiségű, kifinomult támadások indítását, amik túlterhelik a védelmi rendszereket, és nagyobb eséllyel tévesztik meg a végfelhasználókat.

A mesterséges intelligencia lehetővé teszi, hogy a támadók nagyszámú támadást indítsanak, ahol az alacsony sikerességi arány is elfogadható számukra a puszta mennyiségük miatt.

A csalás és az adathalászat folyamatai az automatizációnak köszönhetően sokkal hatékonyabbá váltak, növelve a sikeres végjátékok számát.

Bár a védelmi rendszerek egyre jobban észlelik a fenyegetéseket, az átjutó támadások rendkívül kifinomultak, és nagyobb eséllyel tévesztik meg a végfelhasználókat.



MEGJEGYZÉS: A GRAFIKON BECSÜLT HATÁST ÁBRÁZOL
A LEHETŐSÉG A TÁMADÁSI CÉLPONTOKAT JELZI, A HOOK AZ INDÍTOTT TÁMADÁSOKAT, A JUTALOM A SIKERESEN ÖSSZEGYŰJTÖTT ADATOKAT, A VÉGJÁTÉK PEDIG A SIKERESEN VÉGREHAJTOTT TÁMADÁSOKAT.

Az egyéni bűnözők erőforrásai nem elegendőek ahhoz, hogy olyan nagyszabású csalásokat hajtsanak végre, mint amikor csoportosan és összehangoltan működnek együtt.

Példák a kiberbünözők közötti együttműködésekre:

Strukturált Csapatok: A bűnözői csoportok működésmódja gyakran tükrözi a vállalatok struktúráját specializált szerepkörökkel (pl. rosszindulatú szoftverek, vagy adathalászat).

Információmegosztás: Online fórumok segítségével a kiberbűnözők taktikákat cserélhetnek, megbeszélhetik sebezhetőségeiket, és új tagokat képezhetnek.

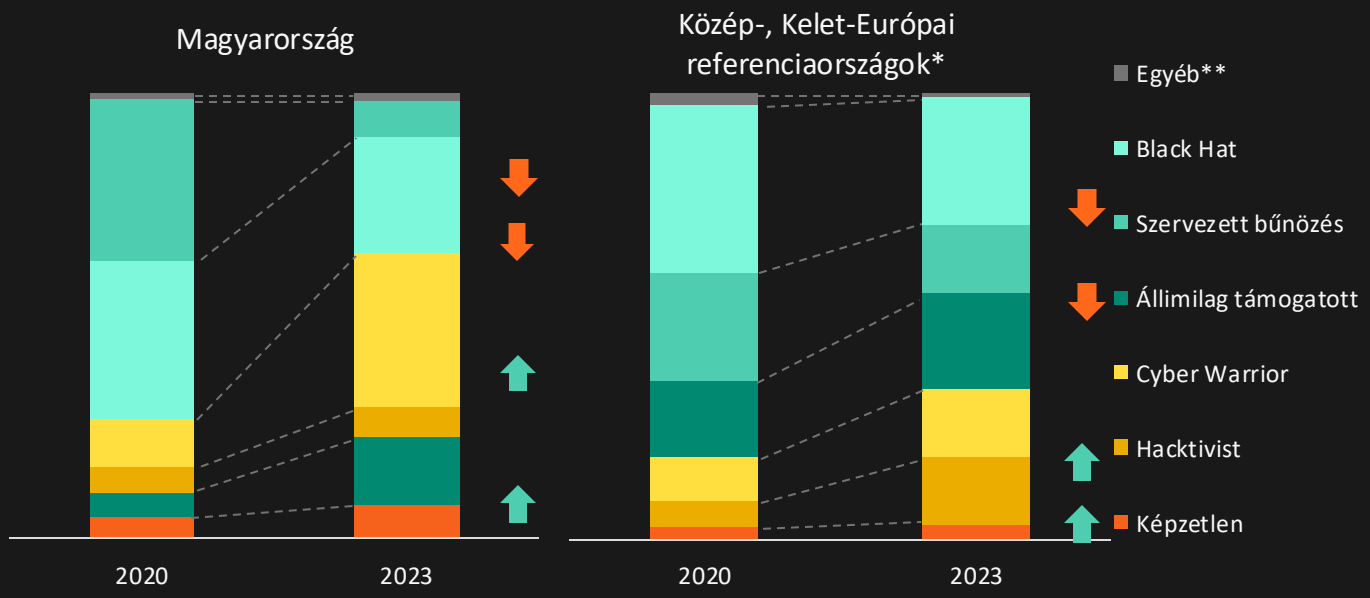
Szolgáltatás Kiszervezés: A bűnözői csoportok az erőforrások és a szakértelem maximalizálása érdekében a speciális feladatokat más képzett elkövetőknek adják ki.

Dark Web Piacterek: A dark web olyan kereskedelmi központként működik, ahol a kiberbűnözők eszközöket, adatokat és szolgáltatásokat vásárolhatnak vagy adhatnak el.

Forrás: [6] Black Hat Middle East & Africa

A magyarországi kibereseményekben több mint fele Cyber Warrior és Black Hat elkövetőkhöz köthető, míg a szervezett bűnözés részvétele jelentősen csökkent.

Kiberincidensek elosztása elkövetői kategóriák szerint



Black Hat (kicsi, független támadói csoportok, amit csak a pénzügyi haszon motivál) elkövetőkhöz kapcsolható a kiberincidensek jelentős része mind Magyarországon, mind a benchmark régióban.

Magyarországon a benchmark országokhoz képest nagyobb mértékben nőtt a **képzetlen elkövetők** aránya, amelynek egyik **oka régiós szinten éppen a technológiai fejlődés**. A mesterséges intelligencia térnyerése alacsonyabbra helyezte a belépési küszöböt a digitális csalások elkövetéséhez, hiszen könnyen automatizálhatóvá, gyorsan adaptálhatóvá és olcsóvá tette a támadásokat.

FORRÁS: [4] MASTERCARD CYBER INISGHTS
NOTE: APPROXIMATE FIGURES, FOR INFORMATIONAL PURPOSES ONLY *AUSTRIA, CROATIA, CZECHIA, HUNGARY, POLAND, ROMANIA, SLOVAKIA, SLOVENIA ** OTHER: CORPORATE SPY, CYBER TERRORISTS, MALICIOUS INSIDER, PRIVILIGED INSIDER

- legalább +/-5 p.p. változás

KiberPajzs
Védelem a pénzügyekben

A magyar lakosság közel sem olyan felkészült, mint amilyennek tartja magát.

Reprezentatív online kutatás a magyar lakosság körében a kiberbiztonsági felkészültségükről:

Minta
Online kérdőíves felmérés (CAWI)

Kvóta
Reprezentatív (nem, kor, település, régió és végzettség)

Célcsoport
18-65 év közötti magyar lakosság

Vizsgált időszak
2024.04.16.-29.

FORRÁS: Reprezentatív kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

KiberPajzs
Védelem a pénzügyekben

Bár Magyarországon a lakosság ismeri a leggyakoribb csalási módokat, a gyakorlatban sokszor rosszul teljesítenek ezeknek a detektálásában.

70%

Egy Mastercard által végzett lakossági kutatás alapján a kitöltők **70%-a szerint nem fordulhat elő, hogy a bank telefonon vagy e-mailben a kártyaadatokat, vagy az online belépési adatokat kéri.** A MÁTRIX projektben összegzett rendőrségi bejelentések mégis több olyan esetet említenek, ahol a sértettektől **10 millió forint feletti összeget csaltak ki ilyen módszerrel.**

60%

A kutatást kitöltők 60%-a ismeri a leggyakoribbnak számító SMS-es adathalászatot, a phishing célú telefonhívásokkal és e-mailekkel pedig szintén több, mint 55%-a találkozott.

46%

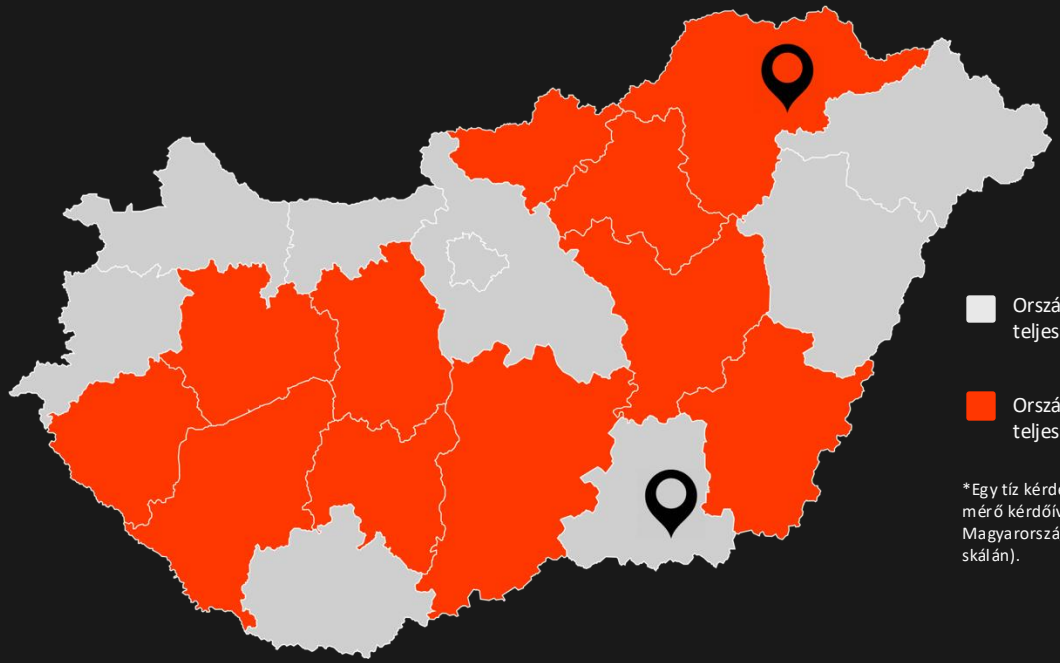
A gyakorlati feladatokban a kitöltők 46%-a azonban **nem tudta eldönteni** a megmutatott üzenetekről, hogy valódiak, vagy csaló szándékúak.

FORRÁS: Reprezentatív kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

KiberPajzs
Védelem a pénzügyekben

Az emberek tudják, hogyan kellene viselkedniük, de nem feltétlenül értik ennek az okát, vagy tudnak ennek eleget tenni.

Digitális index átlaga Magyarországon*



*Egy tíz kérdésből álló elméleti tudást mérő kérdőív átlagos pontszáma Magyarországon 1,86 volt (0-4-ig terjedő skálán).

Az emberek, ha ismerik is a leggyakoribb csalási módokat, elméletben tudják, hogyan védekezzenek ellenük, **nem feltétlenül értik a támadások alapvető működési mechanizmusait, a támadók motivációt és saját pszichológiai sérülékenységüket**.

A digitális index országos átlaga mindössze 1,86 volt (0-4-ig terjedő skálán), a legmagasabb értéket **Csongrád vármegye** érte el mindösszesen **2,10 ponttal**, míg a legkevesebbet **Borsod-Abaúj-Zemplén 1,47 ponttal**.

FORRÁS: Reprezentatív kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

A digitálisan natív fiatalok az online térben való magabiztos navigálásuk miatt túlbecsülik saját kiberbiztonsági ismereteiket, ami kiszolgáltatottá teheti őket, de az idősebbek sincsenek biztonságban.

90,5%

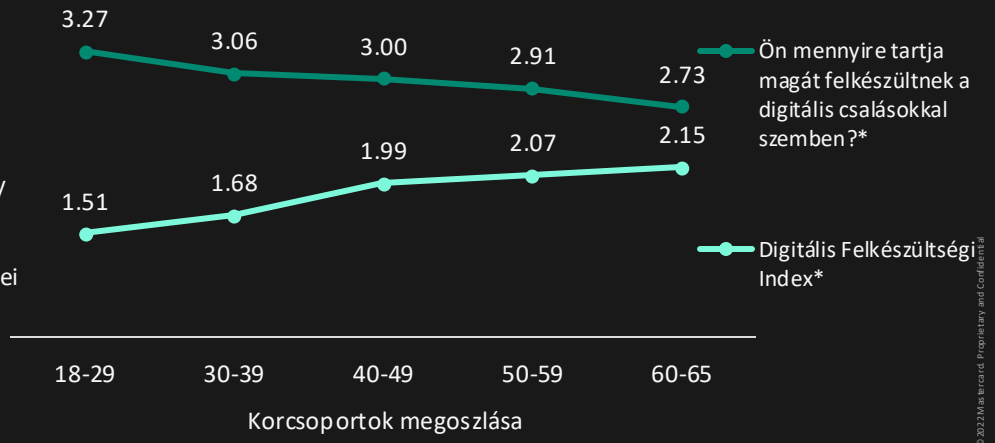
A 18-29 év közöttiek 90,5%-a **tartja magát legalább nehezen átverhetőnek** egy önbevallásos kérdés alapján, amely a kutatás részét képezte.

1,5

Ennek ellenére egy tíz kérdésből álló, elméleti tudást mérő kvízben a 18-29 évesek **digitális biztonsági index átlaga mindössze 1,5** lett (0-4).

42%

A 30-49 év közti középkorú korosztály 42%-a **digitálisan éretlen** az elméleti kérdéssor eredményei alapján.



FORRÁS: Reprezentatív kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

KiberPajzs
Védelem a pénzügyekben

Ismerjük a leggyakoribb módszereket, mégis áldozattá válunk. Jelenleg nem tudunk különbséget tenni csalás és valóság között.

CSOMAGKÜLDÉSES CSALÁSOK

1000 főből közel **70** lakos veszített pénzt

59%-ot ért már ilyen támadás

ebből

11% veszített pénzt vagy adatot

„PIACTÉR" CSALÁSOK

1000 főből közel **90** lakos veszített pénzt

20%-ot ért már ilyen támadás

ebből

43% veszített pénzt vagy adatot

SZOLGÁLTATÓI CSALÁSOK

1000 főből közel **50** lakos veszített pénzt

42%-ot ért már ilyen támadás

ebből

10% veszített pénzt vagy adatot

FORRÁS: 2024 Mastercard U&A felmérés

KiberPajzs
Védelem a pénzügyekben

A szolgáltatói oldal egyre komolyabb nyomással szembesül mind a szabályozók, mind a felhasználók irányából. Egyértelműen szükség van arra, hogy a vállalatok komolyabban és hatékonyabban foglalkozzanak a témával.

53%

A kitöltők 53%-a várna **digitális biztonsággal kapcsolatos tanácsadást a saját bankjuktól**. A 18-29 év közöttiek jelölték a legkevesebben, csupán 49%-uk.

17%

A 18-29 év közöttiek 17%-a várna digitális biztonsággal kapcsolatos információt **saját munkáltatójuktól**.

A NIS2 és a hazai implementációja nagyon jó irány a kiberbiztonság erősítésére, azonban a kisebb vállaltoknak és a lakosságnak is ki kell alakítana ezzel kapcsolatban a maga védekezési startégiáját, mert végső soron az adataik, reputációjuk és pénzük a tét.

Marsi Tamás, Igazgatóhelyettes, NBSZ NKI

Amilyen mértékben nő a szolgáltatói oldalon bekövetkező incidensek száma, úgy fogják ezt mind a felhasználók, mind a szabályozók elvárásai lekövetni. Ez meg fog jelenni a kiberbiztonsági költségvetésekben, valamint tovább fog gyűrűzni a beszállítók irányába is.

Mádi Gábor, CIO, Shiwaforce

FORRÁS: Lakossági kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

KiberPajzs
Védelem a pénzügyekben

A kommunikáció segít, önmagában azonban kevés.

A kutatás legfontosabb megállapításai, amelyek megtalálhatóak bővebben A kiberbűnözés kora 2025 tanulmányunkban:

A **márkák kiberbiztonsági kommunikációjának mérhető hatása van** a fogyasztók digitális biztonsággal kapcsolatos ismereteire.

A kiberbiztonság egyszerűsödése a kommunikációban és a **hamis bizalom kiszolgáltatottabbá teszi az embereket**, hiszen emiatt túlbecsülik saját tudásukat.

A **kiberbiztonsági ismeretek** és **a digitális magatartás között szándék és cselekvés** (intention-action) **szakadék húzódik**.

A fogyasztók feltételezik, hogy **szolgáltatóiknak nagy a felelőssége abban, hogy védőintézkedéseket tegyenek** a védelmük érdekében, és egyre inkább el is várják ezt.

A **fogyasztói élmény (CX) kompromittálása veszélyezteti a biztonságot**, a nem megfelelő UX pedig bizalmatlanságot kelt.

FORRÁS: Reprezentatív kutatás a magyar lakosság körében (Mastercard, Atlas, Rise!, Scale) 2024

KiberPajzs
Védelem a pénzügyekben

A létező kezdeményezéseket támogatnunk, a szektorokon átívelő, szereplőket összekötő kollaborációkat pedig erősítenünk kell.

INFORMÁCIÓMEGOSZTÁS

EGYÉNI KIHÍVÁSOK

Ahhoz, hogy az emberekhez organikusan, a saját közösségi hálójukon keresztül jusson el az információ, **támogatnunk kell a kiberbiztonsági közösségeket, valamint facilitálni, tartalommal feltölteni azokat**.

VÁLLALKOZÓI KIHÍVÁSOK

A szolgáltatók fokozódó nyomással szembesülnek mind szabályozói, mind fogyasztói oldalról. A **felhasználóik hatékony védelme** nem csupán elvárás, hanem üzletileg mérhető faktorrá fog válni.

TECHNOLÓGIA

EGYÉNI KIHÍVÁSOK

Ha a felületeket úgy tervezzük **(usable security)**, hogy a korlátozott ismeretekkel rendelkezők számára is biztonságos felhasználói élményt nyújtsanak, az hatékony lehet.

VÁLLALKOZÓI KIHÍVÁSOK

A szolgáltató feladata, hogy **monitorozza saját és beszállítójának gyengeségeit**, hogy minél előbb felfedezzék a támadásokat, és a lehető leggyorsabban reagáljanak.

OKTATÁS

EGYÉNI KIHÍVÁSOK

A **helyzeti tudatosságra fókuszáló szemlélet** felkészíti a felhasználókat a fenyegetések jobb felismerésére ahelyett, hogy kizárólag elavult rutinokra hagyatkoznának.

VÁLLALKOZÓI KIHÍVÁSOK

Hogy a kibervédelem megerősödjön az ökoszisztémán keresztül, mind munkáltatóknak és felhasználóknak el kell fogadniuk az **együttműködés és helyzeti tudatosság fókuszú oktatást**.

KiberPajzs
Védelem a pénzügyekben

Ha a támadói oldal összefog, tegyünk mi is így. Az országokon és szektorokon átívelő kollaborációkra nagyobb szükség van, mint valaha.

Az online térbe átterelt csalások egyre kevésbé az infrastruktúrát, sokkal inkább a fogyasztót, az embert támadják. Ezen folyamat tudatosítására, visszaszorítására és kárenyhítésére koncentrál a KiberPajzs az idén.

Kovács Levente
Főtitkár
Magyar Bankszövetség

A Kiberpajzs együttműködés és a Nemzeti Kibervédelmi Intézet is folyamatosan frissíti a tartalmait a weboldalukon, valamint folyamatosan azon dolgozunk, hogy a lehető legtöbb csatornán eljuttassuk a kiberbiztonsággal kapcsolatos legfrissebb üzenetet a lakosság felé.

Marsi Tamás
Igazgatóhelyettes
NBSZ NKI

KiberPajzs

A Kiberpajzs célja a magyarországi kiberbűnözéssel szembeni küzdelem, az együttműködés támogatásával, a tudatosság növelésével és felhasználókat segítő kezdeményezésekkel.

A digitális evolúció erősödésével a sokarcú online világban a bűnözők is megjelentek. A KiberPajzs célja, hogy több ezer szakértő tudását összefogva elősegítse, hogy 10 millió magyar ember tudatossága jelentse a masszív védelmet.

Lehetetlen mindenkihez bekopogtatni! Mindannyiunknak ajtót kell nyitnunk a tudásnak – kiélesíteni a szemünket, a fülünket, a figyelmünket!
www.kiberpajzs.hu

Sütő Ágnes, Magyar Bankszövetség főtitkárhelyettes, KiberPajzs társ-projektgazda

A KiberPajzs program összefogja a piaci szereplőket, a jogalkotó és kormányzati szerveket, a védelmi hatóságokat. A közös cél minden oldalról: az ügyfél védelmének és ÖNvédelmének megerősítése – közös edukációval.
Az elmúlt 2 évben 10 milliárd forintnyi médiaértéket összpontosított ismeretterjesztésre, ennek többszörösét a védelem megszervezésére, technológiák fejlesztésére. A KiberPajzs 140 ezer kolléga tapasztalatát, ismereteit koncentrálja, hatalmas intézményrendszerek tudása kapcsolódik össze.

Oktatási kampányok
Partnerségek és együttműködés
Forródrót és bejelentő eszközök
Fokozott biztonsági intézkedések
Áldozattámogatás

KiberPajzs
Védelem a pénzügyekben

A kiberbűncselekményekért valódi büntetés jár!

Ahogy az utcák, otthonok, mindennapok biztonságát adjuk, a rendőrség jelen van az online térben is: **átfogó stratégiát** dolgoztunk ki a kiberbűncselekmények ellen. A kibervilágban új fegyvernemeket kellett kifejlesztenünk. „**Kiber 300**” hálózatunk, új Kiberstratégiai Osztályunk és a Mátrix Projekt, továbbá kiemelt fontosságú edukációs és kommunikációs programjaink. Ütőképes fegyverünk a digitális bűncselekmények visszaszorításában az együttműködés: nemcsak számos szektor – így a bankok - kiberbiztonsági szakértőivel dolgozunk együtt, de jogszabályi változásokat kezdeményeztünk a hatékonyabb hatósági fellépésért, és folyamatos edukációval a lakosságot is bevonjuk a védekezésbe. Élesítjük a harcot a kiberbűnözők ellen!

Töreki Sándor, rendőr vezérőrnagy, bűnügyi főigazgató
országos rendőrfőkapitány-helyettes

KiberPajzs

A Kiberpajzs partnerei:

Magyar Nemzeti Bank
Rendőrség
Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet
Nemzeti Média- és Hírközlési Hatóság
Magyar Bankszövetség
Igazságügyi Minisztérium
Pénzügyi Békéltető Testület
Szabályozott Tevékenységek Felügyeleti Hatósága
Nemzetgazdasági Minisztérium
Magyar Államkincstár
Nemzeti Védelmi Szolgálat
Mastercard
Szerencsejáték Zrt.
Visa

Kommunikációs partner:
Médiaunió

cyber islands

Cyber Islands: Magyarország kiberbiztonsági ökoszisztémájának megerősítése kollaboráción, innováción és megosztott erőforrásokon keresztül

A **Cyber Islands** olyan **kollaborációs csomópontként** szolgál, ahol **a kibervédelmi szakértők, vállalatok, startupok és diákok összekapcsolódhatnak**, innoválhatnak és támogathatják egymást a magyar **kibervédelem fejlesztése érdekében**. A Cyber Islands célja, hogy közös tér és erőforrások biztosításával támogassa az eredményes partnerségek kialakulását és elősegítse a nemzeti kibervédelmi ökoszisztéma növekedését.

A Cyber Islands-et azért hoztuk létre, hogy összefogjuk, inspiráljuk, és egy fizikai helyszínnel támogathassuk azokat a már létező kiberbiztonsági közösségeket, akik jelenleg elszigeteltebben működnek.

Csertán Ákos
Alapító
Cyber Islands

KiberPajzs
Védelem a pénzügyekben

A Cyber Islands célja, hogy a kiberbiztonsági közösségen belül a résztvevők széles körét támogassa, beleértve a következőket is:

Kiberbiztonsági Szakértők

Cégek és Startupok

Diákok és Fiatal Tehetségek

Kiberbiztonság Iránt Érdeklődők

Oktatók és Trénerek

Befektetők

Cyber Islands számos erőforrást es lehetőséget kínál a résztvevőknek, többek között:

Hálózatépítést

Együttműködési tereket

Oktatási erőforrásokat

Közösségi eseményeket

Hozzáférést az eszközökhöz

Karrierépítést

Támogatók: ATLAS, RiSe! Techlabify

Partnerségben: IVSZ SZÖVETSÉG A DIGITÁLIS GAZDASÁGÉRT, WITSEC, Brind, CyberHub Hungary, silent signal, HACKTIVITY, BÁNKI

A kiberbűnözés kora 2025

A kiberbűnözés kora 2025 olyan egyedülálló tanulmány, amely ötvözi a Magyar és Közép-Európai trendeket, meglévő iparági tapasztalatokat, szakértői előrejelzéseket a hazai fogyasztók szükségleteivel.

KiberPajzs

A tanulmány **2025 márciusában** kerül publikálásra együttműködésben a Kiberpajzzsal.